Docket No. AUS920030972US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Brokenshire et al.** § Group Art Unit: **2144**
§
Serial No. **10/763,079** § Examiner: **Anwari, Maceeh**
§
Filed: **January 22, 2004** § Customer No.: **50170**
§
For: **Unidirectional Message Masking** §
and Validation System and Method §
§

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPELLANTS' BRIEF (37 C.F.R. § 41.37)

This Appeal Brief is in furtherance of the Notice of Appeal filed October 1, 2007 (37 C.F.R. § 41.31).

The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying Fee Transmittal.

Real Party in Interest

The real party in interest in this appeal is the following party: International Business Machines Corporation.

Related Appeals and Interferences

With respect to other appeals and interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

Status of Claims

The status of the claims involved in this proceeding is as follows:

1. Claims canceled: 16 and 17
2. Claims withdrawing from consideration but not canceled: NONE
3. Claims pending: 1-15 and 18-23
4. Claims allowed: NONE
5. Claims rejected: 1-15 and 18-23

The claims on appeal are: claims 1-15 and 18-23

Status of Amendments

No amendments to the application were filed subsequent to mailing of the Final Office Action.

Summary of Claimed Subject Matter

Independent Claim 1:

The present invention provides a system in a message source for secure communication. See specification, page 1, line 33, to page 2, line 11; 110 in FIG. 1, for example. The system comprises a random value generator configured to generate a random value. See specification, page 3, line 25, to page 4, line 2; page 8, lines 1-3; 116 in FIG. 1; 200 in FIG. 2, for example. The system further comprises a message validation code generator coupled to the random value generator and configured to generate a message validation code based on a predetermined key, a message, and the random value. See specification, page 3, line 25, to page 4, line 2; page 8, lines 3-8; 118 in FIG. 1; 205 in FIG. 2, for example. The system further comprises a one-time pad generator coupled to the random number generator and configured to generate a one-time pad based on the random value and the predetermined key. See specification, page 3, lines 25-29; page 4, line 3, to page 6, line 10; page 8, lines 9-17; 120 in FIG. 1; 210 in FIG. 2, for example. The system further comprises a masked message generator coupled to the one-time pad generator and configured to generate a masked message based on the one-time pad and the message. See specification, page 3, lines 25-29; page 6, lines 11-16; page 8, lines 17-24; 122 in FIG. 1; 215 in FIG. 2, for example. The system further comprises a transmitter configured to transmit a secure message that comprises the random value, the masked message, and the message validation code to a message target. See specification, page 6, lines 22-25; page 8, lines 31-33; 225 in FIG. 2, for example. The message target is configured to unmask the masked message to form the message and validate the message using the message validation code. See specification, page 6, line 26, to page 7, line 20; FIG. 3, for example.

Independent Claim 7:

The present invention provides a system in a message target for secure communication. See specification, page 1, line 33, to page 2, line 11; 140 in FIG. 1, for example. The system comprises a receiver configured to receive a secure message transmitted from a message source. The secure message comprises a protected message envelope. See specification, page 6, lines 26-31; page 9, lines 1-4; 300 in FIG. 3, for example. The system further comprises a protected message envelope reader configured to receive the protected message envelope and extract a random value, a masked message, and a first message validation code from the received protected message envelope. The random value, the masked message, and the first message validation code are generated at the message source. See specification, page 6, lines 26-33; page 9, lines 5-7; 142 in FIG. 1; 305 in FIG. 3, for example. The system further comprises a one-time pad generator coupled to the protected message envelope reader and configured to generate a one-time pad based on the random value and a predetermined key. See specification, page 7, lines 1-5; page 9, lines 8-13; 144 in FIG. 1; 310 in FIG. 3, for example. The system further comprises a message unmasker coupled to the one-time pad generator and protected message envelope reader and configured to generate an unmasked message based on the one-time pad and the masked message. See specification, page 9, lines 6-10; page 9, lines 13-19; 146 in FIG. 1; 315 in FIG. 3, for example.

Independent Claim 12:

The present invention provides a method in a message source for secure communication. See specification, page 1, line 33, to page 2, line 11; 110 in FIG. 1, for example. The method comprises generating a random value. See specification, page 3, line 25, to page 4, line 2; page 8, lines 1-3; 116 in FIG. 1; 200 in FIG. 2, for example. The method further comprises generating a message validation code based on a predetermined key, a message, the random value, and a first one-way hash function. See specification, page 3, line 25, to page 4, line 2; page 8, lines 3-8; 118 in FIG. 1; 205 in FIG. 2, for example. The method further comprises generating a one-time pad based on the random value and the predetermined key. See specification, page 3, lines 25-29; page 4, line 3, to page 6, line 10; page 8, lines 9-17; 120 in FIG. 1; 210 in FIG. 2, for example. The method further comprises generating a masked message based on the one-time pad and the message. See specification, page 3, lines 25-29; page 6, lines 11-16; page 8, lines 17-24; 122 in FIG. 1; 215 in FIG. 2, for example. The method further comprises transmitting a secure message that comprises the random value, the masked message, and the message validation code to a message target. See specification, page 6, lines 22-25; page 8, lines 31-33; 225 in FIG. 2, for example. The message target is configured to unmask the masked message to form the message and validate the message using the message validation code. See specification, page 6, line 26, to page 7, line 20; FIG. 3, for example.

Independent Claim 18:

The present invention provides a method in a message target for secure communication. See specification, page 1, line 33, to page 2, line 11; 140 in FIG. 1, for example. The method comprises receiving a secure message transmitted from a message source. The secure message comprises the random value, the masked message, and the message validation code. The random value, the masked message, and the first message validation code are generated at the message source. See specification, page 6, lines 26-33; page 9, lines 5-7; 142 in FIG. 1; 305 in FIG. 3, for example. The method further comprises generating a one-time pad based on the random value, a predetermined key, and a one-way hash function. See specification, page 7, lines 1-5; page 9, lines 8-13; 144 in FIG. 1; 310 in FIG. 3, for example. The method further comprises generating an unmasked message based on the one-time pad and the masked message. See specification, page 9, lines 6-10; page 9, lines 13-19; 146 in FIG. 1; 315 in FIG. 3, for example.

Independent Claim 22:

The present invention provides a computer program product for secure communication in a message source. See specification, page 1, line 33, to page 2, line 11; 110 in FIG. 1, for example. The computer program product has a computer readable medium with a computer program embedded thereon. See specification, page 3, lines 8-15, for example. The computer program comprises computer code for generating a random value. See specification, page 3, line 25, to page 4, line 2; page 8, lines 1-3; 116 in FIG. 1; 200 in FIG. 2, for example. The computer program further comprises computer code for generating a message validation code based on a predetermined key, a message, the random value, and a first one-way hash function. See specification, page 3, line 25, to page 4, line 2; page 8, lines 3-8; 118 in FIG. 1; 205 in FIG. 2, for example. The computer program further comprises computer code for generating a one-time pad based on the random value and the predetermined key. See specification, page 3, lines 25-29; page 4, line 3, to page 6, line 10; page 8, lines 9-17; 120 in FIG. 1; 210 in FIG. 2, for example. The computer program further comprises computer code for generating a masked message based on the one-time pad and the message. See specification, page 3, lines 25-29; page 6, lines 11-16; page 8, lines 17-24; 122 in FIG. 1; 215 in FIG. 2, for example. The computer program further comprises computer code for transmitting a secure message that comprises the random value, the masked message, and the message validation code to a message target. See specification, page 6, lines 22-25; page 8, lines 31-33; 225 in FIG. 2, for example. The message target is configured to unmask the masked message to form the message and validate the message using the message validation code. See specification, page 6, line 26, to page 7, line 20; FIG. 3, for example.

Independent Claim 23:

The present invention provides a computer program product in a message target for secure communication. See specification, page 1, line 33, to page 2, line 11; 140 in FIG. 1, for example. The computer program product has a computer readable medium with a computer program embedded thereon. See specification, page 3, lines 8-15, for example. The computer program comprises computer code for receiving a secure message transmitted from a message source. The secure message comprises the random value, the masked message, and the message validation code. The random value, the masked message, and the first message validation code are generated at the message source. See specification, page 6, lines 26-33; page 9, lines 5-7; 142 in FIG. 1; 305 in FIG. 3, for example. The computer program further comprises computer code generating a one-time pad based on the random value, a predetermined key, and a one-way hash function. See specification, page 7, lines 1-5; page 9, lines 8-13; 144 in FIG. 1; 310 in FIG. 3, for example. The computer program further comprises computer code for generating an unmasked message based on the one-time pad and the masked message. See specification, page 9, lines 6-10; page 9, lines 13-19; 146 in FIG. 1; 315 in FIG. 3, for example.

Grounds of Rejection to be Reviewed on Appeal

I. Claims 22 and 23 stand rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the enablement requirement;

II. Claims 22 and 23 stand rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter;

III. Claims 1-15 and 18-23 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by *Shrader et al.* (U.S. Patent No. 6,914,985).

Argument

I. 35 U.S.C. § 112, first paragraph, Alleged Non-Enablement of Claims 22 and 23

The Office rejects claims 22 and 23 under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the enablement requirement. The Final Office Action alleges that the claims contain subject matter that was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. More specifically, the Final Office Action alleges that Appellants fail to point out or describe computer readable media.

Whether the instant specification points out or describes computer readable media is irrelevant, because the rejection alleges that a person of ordinary skill in the art would not have sufficient skill to make or use computer readable media. Appellants respectfully disagree. The instant specification states that the functions described therein are performed by a processor such as a computer or electronic data processor in accordance with code such as computer program code, software, and/or integrated circuits that are coded to perform such functions. See specification, page 2, line 26, to page 3, line 15. Appellants submit that computer readable media, such as floppy disks, magnetic tape, hard disk drives, random access memories, flash memories, optical disks, and the like, are so notoriously well-known that a person of ordinary skill in the art would not require any undue experimentation to store computer code that performs the functions described in the instant specification onto a computer readable medium. Thus, the instant specification sufficiently describes and enables the features of claims 22 and 23.

Therefore, Appellants respectfully request that the rejection of claims 22 and 23 not be sustained.

II. 35 U.S.C. § 101, Allegedly Non-Statutory Subject Matter in Claims 22 and 23

The Office rejects claims 22 and 23 under 35 U.S.C. § 101 as allegedly being drawn to non-statutory subject matter.

With respect to claims 22 and 23, the Final Office Action states that claims 22 and 23 are software *per se* and fail to provide a tangible result. The Examiner alleges that the claims lack a "proper" computer readable medium. Appellants submit that claims 22 and 23 recite a computer readable medium having computer program code. There is no legal, procedural, or logical basis for rejecting claims 22 and 23 based on whether the computer readable medium is "proper." The Examiner proffers no such test; therefore, it is impossible to determine whether claims 22 and 23 pass the proposed test. That is, what is a "proper" computer readable medium? Appellants respectfully submit that computer programs embodied in computer readable media have been held to be statutory and, thus, the Final Office Action is in error. As stated in the MPEP at section 2106 (IV)(B)(1), "[w]hen functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized." As an example, in *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994) a claim to a data structure stored on a computer readable medium that increases computer efficiency was held to be statutory. Claims 22 and 23 recite a computer program embodied on **some** computer readable medium. Whether the Examiner personally finds the computer readable medium to be "proper" is irrelevant.

It is unclear whether the Examiner is interpreting the elements as software *per se* or as software configured to perform an action. Software *per se* cannot perform any action. Software must be executed on some device or structurally tied to some computer readable medium to realize its function. For an example of a system embodiment, the specification states:

> It is further noted that, unless indicated otherwise, all functions described herein may be performed in either hardware or software, or in some combinations thereof. In a preferred embodiment, however, the functions are performed by a processor such as a computer or an electronic data processor in accordance with code such as computer program code, software, and/or integrated circuits that are coded to perform such functions, unless indicated otherwise.

Specification, page 3, lines 8-15. Clearly, a random value generator, for example, cannot be disembodied computer code, because computer code without a device on which to execute or without a computer readable medium cannot provide any function. Therefore, the computer program products recited in claims 22 and 23, for instance, must be computer code that provides functionality when it is executed on a processor, as supported by the specification.

With respect to providing a tangible result, claims 22 and 23 to recite transmitting and receiving, respectively, a secure message. Transmission of a secure message from a message source to a message target provides a concrete, useful, and tangible result.

The Final Office Action states, "[n]owhere in the claims 22 and 23 is it stated that the computer code is 'executed'." However, there is no requirement that the computer code is actually executed. The Examiner appears to be applying personal requirements to the claims that have no basis in law or procedure.

The Final Office Action states, "the claims are not structurally tied to a tangible computer readable media [sic.]." Again, there is no requirement that the computer readable medium be "tangible." What is an "intangible" medium? One cannot make an assumption that Appellants intend to claim imaginary articles of manufacture. If the claim recites a computer readable medium, then the logical assumption is that the claim recites an **actual** real-world computer readable medium. In fact, an intangible medium would be incapable of providing the functions recited in claims 22 and 23; thus, logically claims 22 and 23 must recite a tangible, real-world medium.

Therefore, Applicants respectfully request withdrawal of the rejection of claims 22 and 23 under 35 U.S.C. § 101.

III. 35 U.S.C. § 102, Alleged Anticipation of Claims 1-15 and 18-23

The Office rejects claims 1-15 and 18-23 under 35 U.S.C. § 102(e) as allegedly being anticipated by *Shrader* et al. (U.S. Patent No. 6,914,985). Appellants respectfully traverse this rejection.

A. Claims 1-6, 12-15, and 22

Shrader discloses a method and system for presentation and manipulation of public key cryptography standard (PKCS) enveloped data objects. *Shrader* teaches a data processing system may create, modify, transmit, store, and receive cryptographic data objects formatted according to interoperably defined cryptography standards, such as PKCS #7 EnvelopedData objects. See *Shrader*, col. 6, lines 63-67. *Shrader* generally teaches about digital certificates, public keys, private keys, hash functions, and the like. More particularly, *Shrader* teaches that enveloped data is constructed as follows:

> Enveloped-data is constructed by the following steps:
> 1. A content-encryption key for a particular content-encryption algorithm is generated at random.
> 2. The content-encryption key is encrypted for each recipient. The details of this encryption depend on the key

> management algorithm used, but three general techniques are supported:
>
> key transport: the content-encryption key is encrypted in the recipient's public key;
>
> key agreement: the recipient's public key and the sender's private key are used to generate a pairwise symmetric key, then the content-encryption key is encrypted in the pairwise symmetric key; and
>
> symmetric key-encryption keys: the content-encryption key is encrypted in a previously distributed symmetric key-encryption key.
>
> 3. For each recipient, the encrypted content-encryption key and other recipient-specific information are collected into a RecipientInfo value.
> 4. The content is encrypted with the content-encryption key. Content encryption may require that the content be padded to a multiple of some block size.
> 5. The RecipientInfo values for all the recipients are collected together with the encrypted content to form an EnvelopedData value.
>
> A recipient opens the digital envelope by decrypting one of the encrypted content-encryption keys and then decrypting the encrypted content with the recovered content-encryption key.

Shrader, col. 11, line 45, to col. 12, line 7. Thus, *Shrader* teaches generating an enveloped data object by providing a content-encryption key for each recipient, encrypting the content-encryption key for each recipient, collecting the encrypted content-encryption key and other recipient-specific information into a RecipientInfo value, encrypting the content with the content-encryption key, and collecting the RecipientInfo values for all the recipients with the encrypted content to form an EnvelopedData value.

In contradistinction, with respect to claim 1, for example, the present invention provides a system comprising a random value generator configured to generate a random value. A message validation code generator coupled to the random value generator is configured to generate a message validation code based on a predetermined key, a message, and the random value. A one-time pad generator coupled to the random number generator is configured to generate a one-time pad based on the random value and the predetermined key. A masked message generator coupled to the one-time pad generator is configured to generate a masked message based on the one-time pad and the message. A transmitter is configured to transmit a secure message that comprises the random value, the masked message, and the message validation code to a message target. The message target is configured to unmask the masked message to form the message and validate the message using the message validation code.

With respect to claim 1, the Final Office Action alleges that *Shrader* teaches a message validation code because *Shrader* states that the enveloped data have validation checks. The cited portions of *Shrader* are as follows:

> PKCS #7 describes a general syntax for data that may have cryptography applied to it. In other words, PKCS #7 defines the syntax for several cryptographically protected messages, including encrypted messages and messages with digital signatures. The syntax admits recursion, so that one envelope can be nested inside another or one party can sign previously enveloped digital data. PKCS #7 also allows arbitrary attributes, such as signing time, to be authenticated along with the content of a message, and it also provides for other attributes, such as countersignatures, to be associated with a signature.

Shrader, col. 2, lines 19-29.

> Existing EnvelopedData objects could be dragged and dropped onto the interface to view a preconstructed EnvelopedData object. The interface could also export a EnvelopedData object that passes validation to a file or other transfer mechanism, such as the clipboard, in a DER-encoded format. Before the EnvelopedData object is exported or stored, the interface will run the defined elements through a set of verification rules, presenting errors to the user if present. The same validation checks will also occur when a EnvelopedData object is imported into the interface.

Shrader, col. 13, lines 57-67. Thus, *Shrader* appears to teach attributes to be authenticated and an enveloped data object that passes validation to a file or other transfer mechanism. However, the Final Office Action proffers no explanation as to how this somehow anticipates a message validation **code generator** that is configured to generate a message validation code that is transmitted to the message target and used by the message target to validate the message.

The Office Action alleges that *Shrader* teaches that the message validation code is based on a predetermined key because *Shrader* states how the Public-key cryptography standard is applied within the invention. The cited portions of *Shrader* are as follows:

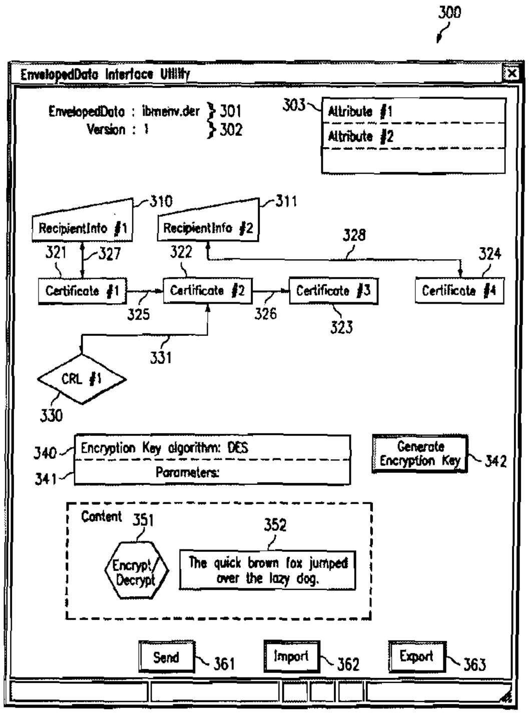
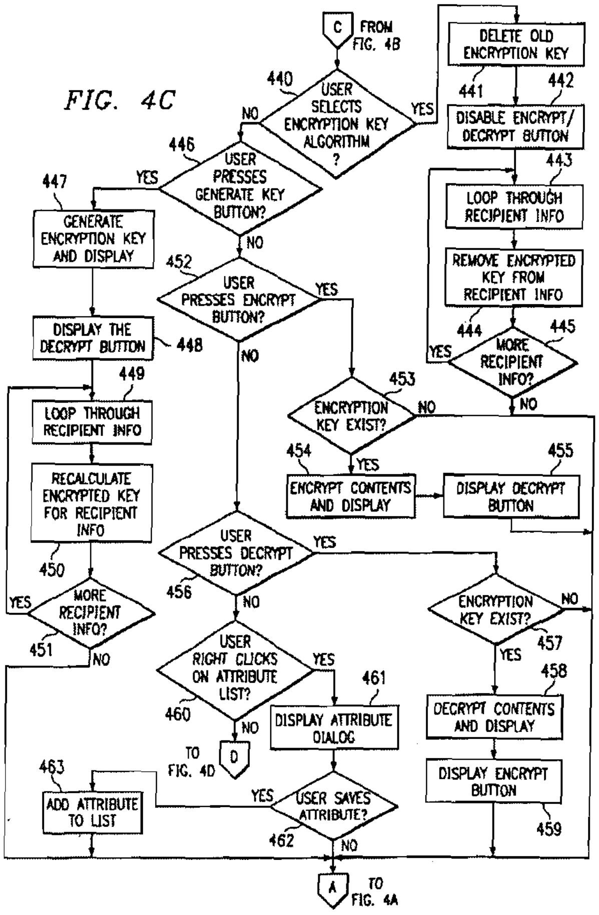
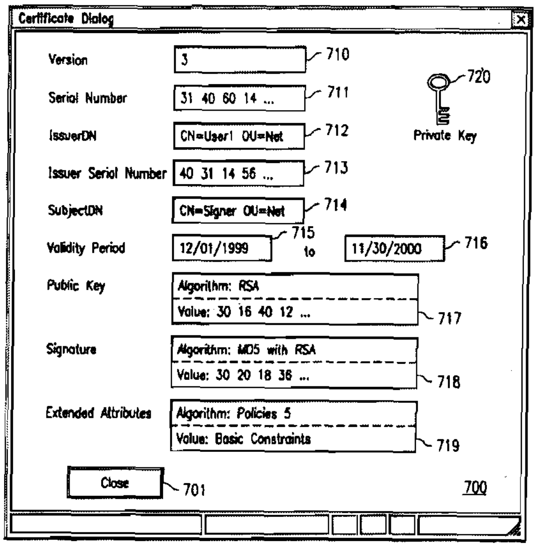

300
EnvelopedData Interface Utility
EnvelopedData : ibmenv.der
301
Version : 1
302
303
Attribute #1
Attribute #2
310
RecipientInfo #1
311
RecipientInfo #2
321
327
322
328
324
Certificate #1
Certificate #2
Certificate #3
Certificate #4
325
326
323
331
CRL #1
330
340
Encryption Key algorithm: DES
341
Parameters:
Generate Encryption Key
342
Content
351
352
Encrypt/ Decrypt
The quick brown fox jumped over the lazy dog.
Send
361
Import
362
Export
363

FIG. 3

FIG. 4C


C
FROM FIG. 4B
440
USER SELECTS ENCRYPTION KEY ALGORITHM ?
YES
NO
DELETE OLD ENCRYPTION KEY
441
442
DISABLE ENCRYPT/ DECRYPT BUTTON
443
LOOP THROUGH RECIPIENT INFO
REMOVE ENCRYPTED KEY FROM RECIPIENT INFO
444
445
MORE RECIPIENT INFO?
YES
NO
446
USER PRESSES GENERATE KEY BUTTON?
447
YES
NO
GENERATE ENCRYPTION KEY AND DISPLAY
DISPLAY THE DECRYPT BUTTON
448
449
LOOP THROUGH RECIPIENT INFO
RECALCULATE ENCRYPTED KEY FOR RECIPIENT INFO
450
MORE RECIPIENT INFO?
YES
451
NO
452
USER PRESSES ENCRYPT BUTTON?
YES
NO
453
ENCRYPTION KEY EXIST?
NO
454
YES
455
ENCRYPT CONTENTS AND DISPLAY
DISPLAY DECRYPT BUTTON
USER PRESSES DECRYPT BUTTON?
YES
456
NO
ENCRYPTION KEY EXIST?
NO
457
YES
458
DECRYPT CONTENTS AND DISPLAY
DISPLAY ENCRYPT BUTTON
459
USER RIGHT CLICKS ON ATTRIBUTE LIST?
YES
461
460
NO
DISPLAY ATTRIBUTE DIALOG
TO FIG. 4D
D
463
ADD ATTRIBUTE TO LIST
YES
USER SAVES ATTRIBUTE?
462
NO
A
TO FIG. 4A



Certificate Dialog

Version: 3

Serial Number: 31 40 60 14 ...

IssuerDN: CN=User1 OU=Net

Issuer Serial Number: 40 31 14 56 ...

SubjectDN: CN=Signer OU=Net

Validity Period: 12/01/1999 to 11/30/2000

Public Key: Algorithm: RSA / Value: 30 16 40 12 ...

Signature: Algorithm: MD5 with RSA / Value: 30 20 18 36 ...

Extended Attributes: Algorithm: Policies 5 / Value: Basic Constraints

FIG. 7

> Public-key cryptography is the technology in which encryption and decryption involve different keys. The two keys are the public key and the private key, and either can encrypt or decrypt data. A user gives his or her public key to other users, keeping the private key to himself or herself. Data encrypted with a public key can be decrypted only with the corresponding private key, and vice versa.
>
> As public-key cryptography has gained acceptance, standards have become necessary so that software at two different sites could work together even when the software is developed by different vendors. In particular, standards have been developed to allow agreement on digital signatures, digital enveloping, digital certification, and key agreement. However, interoperability requires strict adherence to communicable formats, and PKCS, or "Public Key Cryptography Standard," provides a basis for interoperable standards in heterogeneous environments.

Shrader, col. 1, lines 27-43. None of the cited portions teaches or suggests a message validation code generator that generates a message validation code based on a predetermined key, a message, and a random number, as recited in claim 1, for example.

The Final Office Action argues that *Shrader* discloses a validation code based on a predetermined key, a message, and a random value, because *Shrader* allegedly teaches a "digital signature" at col. 13, lines 57-67. The Final Office Action specifically states that a digital signature is a security mechanism that relies on **two** keys that are used to encrypt messages before transmission and to decrypt them on receipt. Clearly, claim 1 does perform a type of encryption when **masking** the message. This is a **separate function** from generating a message validation code. The message validation code does not merely encrypt the message. Rather, the message validation code is a separate value that is transmitted with the masked message. The Final Office Action has not shown where *Shrader* teaches or suggests a message validation code.

Any reference disclosing cryptographic techniques is likely to include words such as "authentication," "key," "hash," and "random" here and there throughout the reference. However, it is the burden of the Office to establish a *prima facie* case of anticipation for the claims, not merely to point to where certain words appear. That is, the Office must address the claim as a whole, demonstrating that the reference teaches each and every claim feature, arranged as they are in the claims. Here, the Office Action appears to cite seemingly arbitrary, albeit lengthy, portions of *Shrader* as allegedly teaching bits and pieces of the claim without explaining how those pieces supposedly fit together to form the present invention.

As a further example, the Office Action alleges that *Shrader* teaches a one-time pad generator that is configured to generate a one-time pad based on the random value and the predetermined key and a masked message generator that is configured to generate a masked message based on the one-time pad, because *Shrader* appears to teach padding encrypted content to a multiple of some block size. However, the Office Action does not explain how padding already encrypted content is somehow equivalent to generating a one-time pad based on a key **and then** masking the message. A person of ordinary skill in the art would not find the teaching of *Shrader* to be equivalent to the invention recited in claim 1, for instance.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.,* 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983).

Applicants submit the Office does not establish a *prima facie* case of anticipation for claim 1. Independent claims 12 and 22 recite features addressed above with respect to claim 1 and are allowable for similar reasons. Since claims 2-6 and 13-15 depend from claims 1 and 12, the same distinctions between *Shrader* and the invention recited in claims 1 and 12 apply for these claims. In addition, claims 2-6 and 13-15 recite further combinations of features not taught by *Shrader*.

With respect to claims 2-6 and 13-15, the Office Action seems to cite more arbitrary portions of the reference simply because the reference uses similar terms. However, Applicants submit that the Office Action does not provide enough explanation as to why the teachings of *Shrader* somehow anticipate the claims. In other words, the Office does not establish a *prima facie* case of anticipation for claims 2-6 and 13-15.

Therefore, Applicants respectfully request that the rejection of claims 1-6, 12-15, and 22 under 35 U.S.C. § 102(e) not be sustained.

A1. <u>Claims 5, 6, 13, and 14</u>

More particularly, with respect to claim 5, for example, the Office Action alleges that *Shrader* teaches a protected message envelope generator that generates a protected message envelope based on the random value, the message validation code, and the masked message, because various portions of the reference allegedly teach a content-encryption key being encrypted at random, attributes to be authenticated, and an encryption messaging process. The Office Action fails to address the claim as a whole. *Shrader* appears to teach pieces of the claimed invention, because *Shrader* is in the same field of endeavor and uses similar terms. However, *Shrader* does not teach the claim features **arranged as they are in the claims**. That is, *Shrader* does not teach generating a random value and generating a message validation code based on the random value, a **predetermined** key, and a message (*Shrader* actually teaches generating a key randomly, not a predetermined key **plus** a random value); *Shrader* does not teach generating a one-time pad **based on the random value and the predetermined key**; *Shrader* does not teach generating a masked message **based on the one-time pad and the predetermined key**; and, *Shrader* does not teach generating a protected message envelope **based on the random value, the message validation code, and the masked message**. Clearly, *Shrader* does not anticipate claim 5, because *Shrader* does not teach each and every claim feature. Claim 13 recites subject matter addressed above with respect to claim 5 and is allowable for similar reasons. Because claims 6 and 14 depend from claims 5 and 13, respectively, the same distinctions between *Shrader* and the invention recited in claims 5 and 13 apply for these claims. In addition, claims 6 and 14 recite further combinations of features not taught by *Shrader*.

With respect to the combination of features in claim 5, the Final Office Action argues that a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. Appellants never argued the "intended use" of claim 5. Rather, Appellants argue that *Shrader* does not teach the combination of features in claim 5 as they are recited in the claim. Therefore, the Examiner's argument about intended use is misplaced and misapplied. That is, the Final Office Action merely argues generally about "intended use" and recites case law, but fails to proffer any explanation as to why or how the argument relates to the teachings of the applied reference with respect to the recited combination of features in claim 5.

Therefore, Applicants respectfully request that the rejection of claims 5, 6, 13, and 14 under 35 U.S.C. § 102(e) not be sustained.

B. <u>Claims 7-15, 18-21, and 23</u>

With respect to claim 7, the Office Action alleges that *Shrader* teaches a protected message envelope reader that extracts a random value generated at the message source, a masked message, and a message validation code from a received protected message envelope, and cites seemingly arbitrary portions of *Shrader* without explanation of how *Shrader* somehow anticipates the combination of features in claim 7. As stated above, *Shrader* appears to teach attributes to be authenticated and an enveloped data object that passes validation to a file or other transfer mechanism. However, the Office Action proffers no explanation as to how this somehow anticipates a message validation **code** that is used by the message target to validate the message. Furthermore, the Office Action does not address how *Shrader* somehow teaches extracting from the enveloped data object a random value that was generated at the message source.

Applicants submit the Office does not establish a *prima facie* case of anticipation for claim 7. Independent claims 18 and 23 recite features addressed above with respect to claim 7 and are allowable for similar reasons. Since claims 8-11 and 19-21 depend from claims 7 and

18, the same distinctions between *Shrader* and the invention recited in claims 7 and 18 apply for these claims. In addition, claims 8-11 and 19-21 recite further combinations of features not taught by *Shrader*.

With respect to claims 8-11 and 19-21, the Office Action seems to cite more arbitrary portions of the reference simply because the reference uses similar terms. However, Applicants submit that the Office Action does not provide enough explanation as to why the teachings of *Shrader* somehow anticipate the claims. In other words, the Office does not establish a *prima facie* case of anticipation for claims 8-11 and 19-21.

Therefore, Applicants respectfully request that the rejection of claims 7-15, 18-21, and 23 under 35 U.S.C. § 102(e) not be sustained.

B1. Claims 9-11, 19, and 20

More particularly, with respect to claim 9, the Office Action alleges that *Shrader* teaches a message validation code comparator that compares a received message validation code with a generated message validation code, because *Shrader* mentions a form of the word "authenticate." Applicants respectfully disagree. Merely mentioning a form of the word "authenticate" is not nearly enough to anticipate the combination of features recited in claim 7, because *Shrader* does not teach a message validation code generator at the message target, a protected message envelope reader that extracts a message validation code from the protected message envelope received from the message source, and a message validation code comparator that compares the message validation code generated at the message target with the message validation code received from the message source. Again, the Office simply fails to establish a *prima facie* case of anticipation for claim 9, for example. Claim 19 recites subject matter addressed above with respect to claim 9 and is allowable for similar reasons. Because claims 10, 11, and 20 depend from claims 9 and 19, the same distinctions between *Shrader* and the invention recited in claims 9 and 19 apply for these claims. In addition, claims 10, 11, and 20 recite further combinations of features not taught by *Shrader*.

Therefore, Applicants respectfully request that the rejection of claims 9-11, 19, and 20 under 35 U.S.C. § 102(e) not be sustained.

Conclusion

In view of the above, Appellants respectfully submit that the features of claims 1-15 and 18-23 are not taught or suggested by the applied prior art. Accordingly, Appellants request that the Board of Patent Appeals and Interferences overturn the rejections set forth in the Final Office Action.

Respectfully submitted,

Stephen R. Tkacs
Reg. No. 46,430
Walder Intellectual Property Law, P.C.
P.O. Box 832745
Richardson, TX 75083
(214) 722-6422
AGENT FOR APPELLANTS

CLAIMS APPENDIX

1. A system in a message source for secure communication, comprising:

a random value generator configured to generate a random value;

a message validation code generator coupled to the random value generator and configured to generate a message validation code based on a predetermined key, a message, and the random value;

a one-time pad generator coupled to the random number generator and configured to generate a one-time pad based on the random value and the predetermined key;

a masked message generator coupled to the one-time pad generator and configured to generate a masked message based on the one-time pad and the message, and

a transmitter configured to transmit a secure message that comprises the random value, the masked message, and the message validation code to a message target,

wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code.

2. The system as recited in claim 1, wherein the message validation code generator employs a first one-way hash function.

3. The system as recited in claim 2, wherein the one-time pad generator employs the first one-way hash function.

4. The system as recited in claim 1, wherein the message validation code generator employs a first one-way hash function and the one-time pad generator employs a second one-way hash

function.

5. The system as recited in claim 1, further comprising a protected message envelope generator coupled to the random value generator, the message validation code generator, and the masked message generator, and configured to generate a protected message envelope based on the random value, the message validation code, and the masked message.

6. The system as recited in claim 5, wherein the transmitter is coupled to the protected message envelope generator and configured to transmit the protected message envelope to the message target.

7. A system in a message target for secure communication, comprising:

a receiver configured to receive a secure message transmitted from a message source, wherein the secure message comprises a protected message envelope;

a protected message envelope reader configured to receive the protected message envelope and extract a random value, a masked message, and a first message validation code from the received protected message envelope, wherein the random value, the masked message, and the first message validation code are generated at the message source;

a one-time pad generator coupled to the protected message envelope reader and configured to generate a one-time pad based on the random value and a predetermined key; and

a message unmasker coupled to the one-time pad generator and protected message envelope reader, and configured to generate an unmasked message based on the one-time pad and the masked message.

8. The system as recited in claim 7, wherein the one-time pad generator employs a first one-way hash function.

9. The system as recited in claim 7, further comprising a validation module coupled to the protected message envelope reader and the message unmasker, the validation module comprising:

a message validation code generator configured to generate a second message validation code based on the predetermined key, the unmasked message, and the random value; and

a message validation code comparator coupled to the protected message envelope reader and the message validation code generator and configured to generate a validation based on the first message validation code and the second message validation code.

10. The system as recited in claim 9, wherein the validation module employs a first one-way hash function.

11. The system as recited in claim 9, wherein the validation module employs a first one-way hash function and the one-time pad generator employs a second one-way hash function.

12. A method in a message source for secure communication, comprising:

generating a random value;

generating a message validation code based on a message, the random value, a predetermined key, and a first one-way hash function;

generating a one-time pad based on the random value, the predetermined key, and a second one-way hash function;

generating a masked message based on the message and the one-time pad; and

transmitting a secure message that comprises the random value, the masked message, and the message validation code to a message target,

wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code.

13. The method as recited in claim 12, further comprising generating a protected message envelope based on the random value, the masked message, and the message validation code.

14. The method as recited in claim 13, wherein the secure message comprises the protected message envelope.

15. The method as recited in claim 12, wherein the first one-way hash function and the second one-way hash function are the same one-way hash function.

18. A method in a message target for secure communication, comprising:

receiving a secure message transmitted from a message source, wherein the secure message comprises a random value, a masked message, and a first message validation code, wherein the random value, the masked message, and the first message validation code are generated at the message source;

generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function; and

generating an unmasked message based on the one-time pad and the masked message.

19. The method as recited in claim 18, further comprising:

generating a second message validation code based on the unmasked message, the random value, the predetermined key and a second one-way hash function; and

comparing the first message validation code to the second message validation code to determine a validity of the unmasked message.

20. The method as recited in claim 19, wherein the first one-way hash function and the second one-way hash function are the same one-way hash function.

21. The method of claim 18, wherein the secure message comprises a protected message envelope, the method further comprising:

extracting the random value, the masked message, and the first message validation code from the received protected message envelope.

22. A computer program product for secure communications in a message source, the computer program product having a computer readable medium with a computer program embedded thereon, the computer program comprising:

computer code for generating a random value;

computer code for generating a message validation code based on a message to be sent, the random value, a predetermined key, and a first one-way hash function;

computer code for generating a one-time pad based on the random value, the predetermined key, and a second one-way hash function;

computer code for generating a masked message based on the message to be sent and the one-time pad;

computer code for generating a protected message envelope based on the random value, the masked message, and the message validation code; and

computer code for transmitting the protected message envelope to a message target,

wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code.

23. A computer program product for secure communications in a message target, the computer program product having a computer readable medium with a computer program embedded thereon, the computer program comprising:

computer code for receiving a protected message envelope transmitted from a message source;

computer code for extracting a random value, a masked message, and a first message validation code based on the protected message envelope, wherein the random value, the masked message, and the first message validation code are generated at the message source;

computer code for generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function;

computer code for generating an unmasked message based on the one-time pad and the masked message;

computer code for generating a second message validation code based on the unmasked message, the random value, the predetermined key, and a second one-way hash function; and

computer code for comparing the first message validation code to the second message validation code to determine a validity of the unmasked message.

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE